Project Overview
This project demonstrates how to deploy a cloud-based honeypot using Microsoft Azure, simulate malicious activity, and monitor/analyze threats using Microsoft Sentinel and Log Analytics. The goal was to learn real-world detection and incident response workflows in a safe environment.

Tools & Technologies Used
- Microsoft Azure
- Windows 10 Enterprise LTSC 2021 VM
- Azure Log Analytics Workspace
- Microsoft Sentinel
- Network Security Group (NSG) rules
- Public IP for external access

Project Steps

1. **Created Virtual Machine**
- OS: Windows 10 Enterprise LTSC 2021
- Size: Standard B1ls (1 vCPU, 0.5 GiB memory)
- Region: East US 2 (Zone 1)
- Public IP: Enabled for external traffic

2. **Configured Networking**
- Deployed NSG to allow RDP, HTTP, and suspicious ports
- Opened ports like 3389, 8080, 445, etc., to mimic vulnerabilities

3. **Log Analytics Workspace**
- Created workspace to collect telemetry
- Connected VM to this workspace via the Microsoft Monitoring Agent

4. **Microsoft Sentinel Integration**
- Enabled Sentinel on the workspace
- Installed built-in analytics rules and threat detection templates

5. **Threat Simulation**
- Simulated external access (e.g., port scans, login attempts)
- Captured activity logs in Sentinel

6. **Analysis**
- Investigated alerts and visualized attacker behavior
- Used workbooks and queries to review incidents

7. **Decommissioned Lab**
- Deleted resources post-analysis to avoid charges